REMARKS

Applicant respectfully requests reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow.

Status of Claims:

Claim 2 is currently being cancelled.

Claims 1, 3, 4 and 6 are currently being amended.

No claims are currently being added.

This amendment and reply amends and cancels claims in this application. A detailed listing of all claims that are, or were, in the application, irrespective of whether the claims remain under examination in the application, is presented, with an appropriate defined status identifier.

After amending and canceling the claims as set forth above, claims 1 and 2-7 are now pending in this application.

Request for Entry of After-final Amendment and Reply:

It is respectfully requested that this after-final amendment and reply be considered and entered, since: a) it is believed to place this application in condition for allowance, and b) at the very least it is believed to lessen the number of potential issues for appeal.

35 U.S.C. § 112, 2nd Paragraph Rejections:

In the Office Action, claims 2 and 4-5 were rejected under 35 U.S.C. § 112, 2nd paragraph, as being indefinite, for the reasons set forth on pages 4 and 5 of the Office Action. In response, claim 4 has been amended to clarify the features recited in that claim, and claim 5 has been amended to address the specific feature in that claim that the Office Action asserted was indefinite.

Claim Rejections – Prior Art:

In the Office Action, claims 6 and 7 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,583,940 to Vidrascu in view of U.S. Patent No. 5,933,501 to Leppek, U.S. Patent No. 6,424,828 to Collins, and U.S. Patent No. 6,907,1234 to Schier; claims 1-5 were also rejected under 35 U.S.C. § 103(a) as being unpatentable over Vidrascu in view of Leppek, Collins and Schier; and claims 1-7 were rejected under 35

U.S.C. § 103(a) as being unpatentable over Vidrascu in view of Leppek, Collins and U.S. Patent No. 6,738,828 to Keats. These rejections are traversed with respect to the presently pending claims, for at least the reasons given below.

Description of Invention:

The present invention relates to a property of an extended address book, i.e., the address, encryption software, an enciphering key, decryption software, and a decryption key, whereby an encryption portion and a decryption portion can be registered in a form whereby they are independent. Such a table structure solves various problems in cryptocommunication.

In the cited art of record, symmetrical cryptocommunication using a database of encryption software is considered in many cases. This database and communicative symmetric property cause various problems. The examples provided below show how asymmetric cryptocommunication and the extended address book of the present invention solves these problems.

Example 1.

In this example, important information, including a customer's personal information etc., cannot be taken out outside of a company. If the significance of the information from a customer is high, it will be enciphered and the information from a customer will reach a company. It is not realistic that the management receives and processes all code mails in this form from a customer. After personnel receive and process the mail enciphered from the customer, it is realistic to report a required point to the management.

In order to prevent personnel carrying out customer data in the company to an external source (e.g., outside the company), this example forbids transmitting the information as which personnel were enciphered to externally (e.g., outside the company), and that code mail that can be transmitted externally can consider a case where it is made only to the management.

In this case, an office worker's mailer must be able to be set up and not encipher the information to transmit, although the received code mail must be able to be decrypted.

The present invention solves the problems with the example provided above by separating an encryption portion and a decryption portion and treating them independently.

Along these lines, since the code mail from personnel is not sent to the mailer of the visitor who transmits code mail to personnel, encryption software and an enciphering key are registered into personnel's line (row) of a visitor's address book, but the column of decryption software and a decryption key is set to a blank.

Although the column of encryption software and an enciphering key of the line about this visitor of personnel's address book is set to a blank, decryption software and a decryption key are registered in the present invention.

Example 2.

In this example, enciphered communication networks (telephone networks, etc.) are considered. The function of the telephone and computer which can be used with it improves rapidly in each passing year.

In more detail, present day computers have a powerful calculation function. However, even if a new telephone and a new computer are put on the market, some users of cryptocommunication can purchase it immediately, and other users will not purchase it until many years later (e.g., 10 years from now).

The present invention addresses a case in which an old telephone and an old computer having a not-so-powerful calculation function are used in a network.

Suppose that Mr. A, Mr. B, and Mr. C are the members of a cryptocommunication network. Although Mr. A and Mr. B have the latest (and most powerful) computers, Mr. C still uses an old computer having less computational power.

Although Mr. A communicates with Mr. B and Mr. C, he presupposes that Mr. B communicates only with people with new computers.

In order for Mr. A and Mr. C to perform cryptocommunication smoothly, they must be able to adopt an easy cipher system suitable for the limited computational power of the computer which Mr. C has. This is because a decryption will take too much time by Mr. C's computer if a powerful encryption is chosen, which will adversely affect a telephone call between Mr. C and either Mr. A or Mr. B.

A code database becomes practically useless for people who do not perform communication with those who have old computers among people with more recent (and more powerful) computers. It is a waste of memory to save the old software which is not used by the new computers.

Since memory can be utilized effectively by supposing it performs cryptocommunication only by those who have computers and telephones of the latest style except for Mr. C, more powerful encryption can be used. However, a communication network will be destroyed whenever a newer telephone and computers are connected onto the network, if Mr. C is excluded.

In this case, the members of the network should not utilize a method using a common encryption software, and each user should manage encryption software uniquely. It should be made to use what suits Mr. C and what suits Mr. A.

The following is done to achieve more powerful communication by encryption. If both members of a telephone call have a machine (telephone and computer) of high performance, a powerful code can be used, and if at least one of the members of the telephone call has an old machine, only an easy code should be used in that case.

Therefore, Mr. A's address book is as follows:

The encryption software of Mr. B's line is powerful, and an enciphering key will become long. Of course, the decryption software of Mr. B's line is powerful, and a decryption key will become long. Of course, the software which uses another cryptographic algorithm may be sufficient as encryption software and decryption software.

An easy encryption software and enciphering key of Mr. C's line is registered in Mr. A's address book. Of course, the decryption software of Mr. C's line is easy, and a decryption key will become short. Also, the software which uses another cryptographic algorithm may be sufficient as encryption software and decryption software.

Accordingly, Mr. C has to register only easy encryption software into his own computer altogether according to his own old computer.

Therefore, Mr. C's address book is as follows:

Since Mr. B and Mr. C do not communicate, Mr. B's line does not exist in Mr. C's address book.

An easy encryption software of Mr. A's line and a short enciphering key is registered. Of course, the decryption software of Mr. A's line is easy, and a decryption key will become short. Also, the software which uses another cryptographic algorithm may be sufficient as encryption software and decryption software.

Since Mr. B's communications partners are only people with the newest powerful machinery, all the encryption software registered into Mr. B's machinery is of the latest and

most powerful type. It is not necessary to put the old software into Mr. B's machine since it is not used on its own computer (and since Mr. B does not communicate with Mr. C and others who have old computers).

Therefore, the extended address books differ in Mr. A's, Mr. B's, and Mr.C's respectively, and it is obvious they are unrelated to a common database.

The Rationale for Building a Database of Encryption Software and Unifying Encryption Software as a Whole

When renewal of a database becomes difficult, deciding whether old encryption software is to be discarded with or updated according to the computational power of machinery on a network, a method that banishes people with old machinery from a cryptocommunication network must be chosen. Though added, if it does not perform discarding, unnecessary encryption software will be kept in large quantities in the database, and memory space will be used unproductively.

It becomes clear from Example 3 below that renewal of a database and unification are very difficult subjects. However, since a structure in which an encryption column and a decryption column can set up freely for every communications partner existing in a network is utilized in accordance with the present invention, both persons having the latest computers and telephones and persons having old versions of computers and telephones can live together and communicate with each other in a cryptocommunication network.

Example 3.

There is a still more difficult problems in a code database. One problem is the limit concerning the activity of a code.

There is a big difference in the policy about cryptocommunication from country to country. For example, a country which is not allowed to transmit although it is possible to receive information from a country which can perform communication enciphered freely. Although a country which allowed neither transmission of the enciphered data nor reception and the activity of a code is permitted on a network, other countries where a limit is attached to the treatment of an algorithm, an enciphering key, and a decryption key is varied.

This cries out for uniformity amongst different countries, since it is common that communications crosses borders of countries.

For example, as long as mechanical capacity allows, cryptocommunication should be carried out to a friend who lives in a country which uses an enciphering key of the length in the limit to those who live in the country where a limit is attached to the length of a key, especially those that do not have a limit using a long key for making a powerful code.

It will be more severe when those who live in the country which asks for presentation of an enciphering key and a decryption key participate in this cryptocommunication network. It is because the person of the position which can decrypt all the codes registered into the code database will exist when the information on the accumulated key flows out.

Though the law of each country is protected, in order to realize the safest possible communication, the present invention allows ones to manage their own address book freely, and register the optimal encryption software. Also, only the part of those who do cryptocommunication directly with themselves is managed. Even if hacking of a certain person's computer is carried out, there is little influence on the whole cryptocommunication network. People who perform direct communication with the person by whom cracking was done should transpose only people's line by which cracking was carried out to new software and a new key.

Vidrascu Reference:

a. Column 6, lines 21-31 of Vidrascu:

This portion of Vidrascu describes that when IP data transmission transporting a TCP or UDP protocol is received (normally plane) on the interface 30 (see Figure 1 of Vidrascu). If the keys related to the IP addresses of the sender and of the receiver are found, a part of the user data of this transmission is enciphered with a DES algorithm by using a key related to the IP address of the sender.

The transmission is next sent to the interface 31. When an IP data transmission transporting a TCP or UDP protocol is received (normally enciphered) on the interface 31, and if the keys related to the IP address of the sender and of the receiver are found, a part of the user data of this datagram is decrypted with a DES algorithm by using a key related to the IP address of the sender (the same key as that having served in the enciphering). The datagram is next sent to the interface 30.

In 1986, there became the use of the mail structure of "User@domain" form. IP address corresponds to "domain" after the mark "@". Therefore, both "user11@domain1" and "user12@domain1" belong to the same mail server which have a same IP address.

Moreover, "user21@domain2" and "user22@domain2" also belong to the same mail server with a same IP address, and also from "user11@domain1" to "user21@domain2". The same encryption is done in the communication from "user11@domain1" to "user21@domain2" and the communication from "user12@domain1" to "user22@domain2".

There are many people using the same IP provider, and the users using the same IP address increase in number inevitably. Therefore, with the same method and the same enciphering key, a lot of data will be enciphered and it will be transmitted. This becomes a big factor by which a code will be decoded.

The response between IP addresses means the response between mail servers. Thus, it will be only via a manager of a mail server that encryption software can be changed. There are many people using the same provider's mail server. The group of the people using two mail servers will use the same encryption software. Now, each user of an E-mail cannot change encryption software freely, since it must be able to change.

In order for the user of an e-mail to choose the encryption software which suits that user and to use it freely, encryption software and an enciphering key must be able to be set up not according to the response of an IP address and an IP address but according to the response between mail addresses. If the user purchases new machinery (e.g., new telephone and computer), the user should enable it to change into a stronger and more robust code. If this is not made, cryptocommunication with those who live in foreign countries where legal limits differ may cause problems. For realizing communications with people of various countries registered into their own address book, and smooth cryptocommunication, the user of an e-mail has to be able to set up freely in the user's own address book.

Vidrascu does not teach or suggest choosing the key of a code to compensate for an IP address set and choosing encryption software as an IP address. The encryption software which appears in Vidrascu is only DES, and description which uses the code of an algorithm which it is at the transmission (to the same partner) and reception time from the same partner, and no differences exist.

Vidrascu's method includes additional problems. This is with respect to a boundary point of a safe network and a network which is not safe, and trying to perform encryption and a decryption on that boundary. The problem is whether the local network made safe exists. For example, the customer data of a company are sold and bought at a high price. A possibility of intercepting an unenciphered packet containing personnel information which is flowing in the local network made safe, and thereby being unlawfully sold outside the company has to be fully considered. Most leaks of information are the forms where employees of a company makes confidential information flow external to the company. Therefore, the boundary of a safe network and a network which is not safe does not exist in that circumstance. Thus, data needs to be enciphered when coming out of a user's own personal computer. Therefore, management of encryption software must be directly carried out with each personal computer, and everybody needs to have an address book extended into its own personal computer.

b. Column 12, lines 1-11 of Vidrascu

In this portion of Vidrascu, if first and second keys exist, enciphering a message is enciphered to be sent with the first key to obtain an enciphered message, and the enciphered message is transmitted by the sending equipment of the first item of equipment, and otherwise the message is not sent (e.g., rejected). This portion of Vidrascu also describes verifying a presence of a second memory card to authenticate a second operator of the second item of equipment; and if the first and second keys exist, deciphering a received message with the second key and otherwise reject a received message.

The problems with this scheme are as follows. The first key is used for the encryption at the time of transmission, and the second key is used for the decryption in the side which receives the enciphered data. Suppose that Mr. A sends data enciphered to Mr. B. Even if Mr. A checks that the 1st key and 2nd key are in their place, it does not mean having checked that the 2nd key was in Mr. B's place. Even if Mr. B is telephoned and a check is performed before Mr. A's transmitting, a judgment as to whether Mr. B is really the recipient cannot be performed. Rather, Mr. A has to go to Mr. B's place before transmission, and he has to check existence of the 2nd key by himself.

Also, in international communication, such a scheme is not used.

First of all, it is not necessary to investigate the 2nd key that cannot be checked. Rather, it will encipher and send if there is the 1st key. If it does not arrive correctly, there is a notice sent from Mr. B.

The checking performed here is not checking existence of encryption software, rather it is checking of only an existence of a key. It is an item which must be checked if it may not encipher as the case where uses of many kinds of encryption software. This is because Vidrascu does not consider that encryption software considers only DES.

If change of encryption software is to be considered, the description about whether what one will do with change and registration of encryption software by who determining in what kind of position will be required. Such features are not taught or suggested by Vidrascu.

Four things need to be considered if one is to consider a key.
1. Key used when enciphering data which Mr. A sends to Mr. B.
2. Key used when Decrypting Data which Mr. B Received from Mr. A.
3. Key used when Enciphering Data which Mr. B Sends to Mr. A .
4. Key used when decrypting data which Mr. A received from Mr. B.

Encryption software is also the same, and has four things to consider.
1. Software used when enciphering data which Mr. A sends to Mr. B.
2. Software used when decrypting data which Mr. B received from Mr. A.
3. Software used when enciphering data which Mr. B sends to Mr. A.
4. Software used when decrypting data which Mr. A received from Mr. B.

By the method according to the present invention, on the contrary, it does not carry out checking existence of a certain thing to a remote place. This is because it does not perform certification of existing software even if suitable in the past.

Rather, in the present invention, it is an enciphering key and the encryption software which are checked at the time of transmission. This is because those who return only the data which is not enciphered are also needed even if there is received code data.

Naturally at the time of reception, only existence of a decryption key and decryption software is considered. This is because the data enciphered to a person may be unable to be transmitted even if the enciphered data is receivable from the person. The existence of a country by which hacking or other unlawful things may be carried out only by receiving the enciphered data is also considered.

Returning back to Vidrascu, when it decides to use the cipher program of a public key system, a major problem arises. In a public key system, the 2nd key is a secret key and it is not sent out to a sending person. This method cannot be equivalent to a public key system. A

system such as Vidrascu's that cannot respond to a public key system is already an outdated system.

Schier reference:

a. col. 9 line 67 to col. 10 lines 1-7 of Schier:

In this portion of Schier, a receiving device 78 includes a copy of table 80. The copy of table 80 is then used at step 132 to retrieve the first indicated encryption algorithm from the encryption algorithm column 84. This encryption algorithm is then loaded into the encryption decryption engine 30 and is executed by central processing unit 20 to encrypt outgoing communication and decrypt incoming communication at step 134.

One problem of Schier is having a copy of table 80. It is that the decryption software specified by the same number as the encryption software specified by the number of the encryption algorithm indicated on the table exists in both device 78 and device 72.

For example, Mr. B and Mr. C will also have the same table, and all the members will have the same table. It contains a problem in some respects that those that participate in a cryptocommunication network need to have a common table.

Using a copy will share the same encryption software as the table with all the same machinery that participates in this cryptocommunication network, and the same decryption software.

Since this encryption communication network accepts intervention of outdated machinery, weak encryption which is used also by low processing performance machines will be used.

Since all the machinery has a copy, if the number of the machinery which participates in the encryption communication network increases, changing into new cryptographic algorithm will become very difficult. This is the case because there are those who can pay the royalty of encryption software or decryption software, and those who cannot pay, and the law of a different country may allow the activity of the algorithm, or may not be allowed. There are some countries which have forbidden carrying out powerful encryption software abroad, and there are also some countries which have allowed carrying out freely. If a copy is distributed on the Internet, it may become a criminal act in those countries in many cases.

Also, consider the following case. Codes can be freely used in the country where Mr. A lives. However, in the country Mr. B lives, when receiving, the codes can be freely used as

well as Mr. A, although there is a limitation which only an easy encrypting scheme can be permitted on transmitting.

So, in the country of Mr. B, the encryption software should be easy and with a short enciphering key.

If the table and encryption software of encryption of Mr. A are sent to Mr. B, he will be an offender only by Mr. B using it. In order to build as effective a cryptocommunication network as possible in this system, the extended address book (telephone number book) which everybody manages uniquely is required.

There may also exist a country which requests submission of a decryption key to the public institution of that country. If the copy of a code database is used, the country which submitted the key can decode all the communications. Since the information on such an accumulated decryption key and an enciphering key can be sold at a high price, worries about the leak of information from that public institution of the country also takes place. If those that participate in a network share encryption and decryption, it will have the capacity which all the members can decode.

For the above reason, this method of Schier is not fit for international communication, since a copy must be given up. However, this difficulty is solvable if the feature of an address book in accordance with the present invention is used.

Encryption software is divided into an encryption portion and a decryption portion, and to extend an address book in the form suitable for it, and to have it enabled to register encryption software, an enciphering key, decryption software, and a decryption key are needed to be stored. This point is not described at all in Schier.

In accordance with the present invention, assume that Mr. A and Mr. B buy new telephones, and suppose that Mr. C continues to use his old telephone. By way of the present invention, the encryption software and enciphering key which are registered into the line of Mr. B of the address book of Mr. A can register the newest encryption software, and can thereby use it.

Since Mr. C has only an old telephone, also when performing cryptocommunication with Mr. A, and also when performing cryptocommunication with Mr. B, he uses an easy cipher system. Since a decryption and encryption take too much time to perform by Mr. C's

old telephone, a powerful new code cannot be used. Therefore, an old, easy encryption software is registered into the line of Mr. B of the address book in which Mr. C was extended.

Therefore, the address book in which Mr. A was extended, and the address book in which Mr. C was extended are different, and are not copies of each other. This is unlike the features of Schier.

Leppek Reference:

Col. 2, lines 19-23, 51-55, and Col. 4, lines 14-17 of Leppek:

Leppek describes a virtual encryption scheme that involves the generation of a sequence of the access code, with immediately successive ones of the access code of the sequence being different from one another. Col. 2, lines 51-55 describes that the order of the encryptors within the sequence to which the data is applied may very as desired, and the sequence may 'toggle' or switch back and forth between the same set of encryption operators as part of its overall encryption flow. Col. 4, lines 14-17 describe that the encryption routines 110, in and of themselves, need not be any particular type of encryption algorithm and may be conventional encryption operations, such as PGP, DES, etc. routines, as non-limiting examples.

There are many problems with the method of Leppek.

1. Is Database Common to All the Members?

If common, how is the problem of copyright and an illegal copy solved?

How do an economic discrepancy and a legal wall exceed?

If not common, how does the algorithm which makes a number from a key correspond to this unbalance?

2. Isn't there any limit in table size?

When changing the length of an enciphering key with the same algorithm, what does it do?

In key RSA which becomes long very rapidly, it is likely that there will be about 8000 bits in the near future, as there is at present a 2048-bit key.

It becomes practically impossible for the length of the table of a database to become the 8000th power of 2, and to manage that whole database.

3. Is Soft New Addition Possible?

4. Is Old Soft Deletion Possible?

5. Is Rewriting Possible?

6. What Happens to Determination of Number after Change?

7. What Does ENCR.KEY Use?

As seen from the problems above, there should not be used a database which manages the whole system. Also, everybody must be made to have to manage only a part to use for one's own communication. Further, everybody manages the address, encryption software, an enciphering key, decryption software, and a decryption key for every communication partner.

In contrast, the method based on an own extended address book according to the present invention is relatively simple for registration and updating, and overcomes the problems associated with Leppek.

Collins Reference:

a. col. 5, lines 43-63 of Collins:

In Collins, an Internet e-mail gateway 240 converts an SMS message 100 to an Internet e-mail message having the format 150. To accomplish this, the Internet e-mail gateway 240 determines an Internet e-mail address for the cellular telephone 210 and for the Internet station 280. Regarding the Internet e-mail address for the cellular telephone 210, the Internet e-mail gateway 240 adds the domain name for the Internet e-mail gateway 240 to the SMS address for the cellular telephone located in the sender SMS address field 110 of the SMS message. To determine the Internet e-mail address for the Internet Station 280, the Internet e-mail gateway 240 uses a messaging service lookup table having a first column with a list of SMS addresses, where each SMS address corresponds to an Internet e-mail address in a second column of the lookup table. The Internet e-mail gateway 240 locates the SMS address of the Internet station 280 in the first column of the lookup table. The Internet e-mail address for the Internet station 280 is retrieved from the second column of the lookup table at a location corresponding to the Internet station SMS address of the first column.

In Collins, the response relation between the SMS address and an internet mail address is only described.

There is no description of use of an extended address book in the system and method of Collins.

Keats Reference:

In Keats, each network element has its own SID (maintained for example in a memory element under control of the SID manager) and also maintains a database, table or other suitable structure in another memory element, such as a cache, which maps TIDs to IP address for IP connections from the particular network element to another network element in the network, as described in detail below.

There is no description of use of an extended address book in the system and method of Collins.

Comments in "Response to Amendments" Portion of Office Action:

In response to the comments made in section 8) of the Office Action, claim 1 has been amended to explicitly recite the features that the Examiner asserted were not present in claim 1.

In response to the comments made in section 13) of the Office Action, claim 3 has been amended to recite "application order data indicating an order in which each of the pairs of the enciphering key and the enciphering software is applied."

In response to the comments made in section 15) of the Office Action, claims 3 and 4 have been amended to clarify certain features recited in those claims.

In response to the comments made in section 16) of the Office Action, claim 6 has been amended to clarify certain features recited in those claims.

Prior Art Rejection of Claims based on combination of Vidrascu, Leppek, Collins, and Schier:

Vidrascu describes cryptocommunication between IP address. A communication network which is safe and a communication network with is not safe are divided and considered. The number of cipher systems currently treated is one, and there is performed checking for further existence of a key used for a decryption by a receiving side at the time of transmission.

Leppek describes a method which uses a database treating multiplex encryption of encryption software.

Collins relates to a response of an SMS address internet mail address.

Schier relates to sharing the copy of a table 80 in which telephone numbers are registered with the table. Such a table is practically meaningless for real-world implementation and is not realistic.

Vidrascu and Schier relate the sharing of a common database, which is totally unlike the present invention.

Vidrascu has described a method of cryptocommunication, but such method is much different from the present invention (see discussion of Vidrascu above) and has many problems that do not allow for safe communication.

Namely, the following problems exist in Vidrascu's method:

1. The path length into which the signal which is not enciphered flows is not the shortest.

In the network made safe, the data which is not enciphered flows and it is enciphered on a boundary line with the network made not safe. The place which assumes the existence of a network recognized safe is the biggest trouble. It is the feature of a present-day information crime which information reveals from human being inside an organization in many cases.

2. It is enciphered using an algorithm with much the same data.

In the structure of an E-mail, many mail addresses correspond to the same IP address. Many people using one mail server are using the same IP address.

Therefore, when a cryptocommunication network is built based on the response of an IP address and an IP address, many E-mails will be enciphered by the same method. This serves as a big key of decryption.

3. A hacker tapping into the system can also encipher the data which he made by the common method.

If a hacker registers himself as a user of the mail server made into the purpose, the data which is useful for decryption will be transmitted, the feature of an algorithm will be caught, and a possibility of succeeding in performing an unlawful decoding will become high.

4. There is a problem in the determination of the encoding technology to be used.
5. There is a problem in changing the encoding technology to be used.
6. A problem in difference in the laws of different countries.

The above problems are solvable by the method of the present invention.

1. Data is enciphered when coming out of a personal computer. The enciphered data is decrypted in a personal computer. Therefore, the communication path into which the data which is not enciphered flows does not exist.

2. It is enciphered using the algorithm with which much data differs.

By the present invention, if economical and technical conditions allow, different encryption algorithms to the group of each sending person's mail address and an addressee's mail address can be used.

3. The hacker cannot encipher the data which he made by the method.

A hacker is unable to obtain various data enciphered by the communication path by the method, since the method of encryption is unknown to the hacker.

4. Determination of the encoding technology to be used can be performed in judgment of an individual.

5. Change to the encoding technology to be used can be performed freely.

The encoding technology which is not reliable can be thrown away immediately and can be freely changed into a new technology.

6. A fine response is made to the differences in the laws of different countries.

Since the present invention can set up independently for every mail address the case of transmission, and in the case of reception, cryptocommunication can be used by the method of the present invention suitable for the law of the country in which the communications partner lives.

These became possible because there is managed uniquely an extended address book that has an item of the address, encryption software, an enciphering key, decryption software, and a decryption key, and the extended address book.

Accordingly, a firm cryptocommunication network can be built by using the encryption software divided into the encryption portion and the decryption portion in accordance with this. A common code database is not utilized in the present invention.

Each of the Comments made in the Prior Art Rejection section of the Office Action will be addressed in detail below.

Regarding Section 18:

In column 6, lines 21-31 of Vidrascu, when IP data transmission transporting a TCP or UDP protocol is received (normally plane) on the interface 30 (See Figure 1), and if the keys related to the IP addresses of the sender and of the receiver are found, a part of the user data of this transmission is enciphered with a DES algorithm by using a key related to the IP address of the sender. The transmission is next sent to the interface 31. When an IP data transmission transporting a TCP or UDP protocol is received (normally enciphered) on the interface 31, and if the keys related to the IP address of the sender and of the receiver are found, a part of the user data of this datagram is decrypted with DES algorithm by using a key related to the IP address of the sender (the same key as that having served in the enciphering). The datagram is next sent to the interface 30.

An enciphered program is in interface 30, a decryption program is in interface 31, it is a talk in the case of decrypting what was enciphered with interface 30 with received interface 31, and the existing place is different.

The response is not considered as the place of interface 30 is equipped with an enciphered program and a decryption program. Since it stands to reason that it is decrypted after the enciphered data is received, the necessity that the address, encryption software, an enciphering key, decryption software, and a decryption key must be added to the item of a table from this idea does not come out from the teachings of Vidrascu.

Since DES is a symmetrical key method, the key is common in such a system. Two keys are investigated also in the time of transmission. Two keys are investigated also in the time of reception. This means that the reply to A from B is similarly enciphered by DES because two keys exist, when the transmission to B from A is enciphered by a DES method. Also, even if it investigates that the same key exists in two hands, it is meaningless because it is enciphered using the same key.

Accordingly, these teachings of Vidrascu are much different from the presently claimed invention.

In column, 12, lines 1-11 of Vidrascu, if the first and second keys exist, enciphering a message to be sent with the first key to obtain an enciphered message, and transmitting the enciphered message by the sending equipment of the first item of equipment and otherwise rejecting the message to be sent.

The checking that is performed here in Vidrascu is not checking existence of encryption software, but rather checking only an existence of a key. If change of encryption software is considered, the description about whether what we do with change and registration of encryption software by who determining in what kind of position will be required. Vidrascu does not address these points at all.

Note that there are "keys" in the plural form. If transmission and reception are separated, the number of keys required for encryption of transmission will be one. Only existence of an enciphering key and encryption software should be considered at the time of transmission.

In stark contrast to the method of Vidrascu, in the present invention, it is an enciphering key and the encryption software which are checked at the time of transmission. Naturally at the time of reception, only existence of a decryption key and decryption software is considered. This is because the data enciphered to the person may be unable to be transmitted even if the enciphered data is receivable from the person. The existence of a country by which offender treatment will be carried out only by receiving the enciphered data is also considered.

In column 6, lines 23-27 of Vidrascu, if the keys related to the IP addresses of the sender and of the receiver are found, a part of the user data of this transmission is enciphered with a DES algorithm by using a key related to the IP address of the sender. This falls well short of the features recited in the presently pending claims under rejection.

Turning now to Schier, Figure 3 and Figure 6 of Schier show the response of encryption software that is written to be a key (place which can be interpreted as the telephone number). The portion of an enciphering key is required and the item of decryption software and a decryption key is further required. Without these items, not every user of an E-mail can use encryption software freely, and the user cannot promptly respond to either the difference in the law for every country, or the difference in the rules for every organization.

Column 10, line 1 and column 9, line 67 to column 10, lines 1-7 of Schier describe a receiving device 78 that includes a copy of table 80. This means that the whole system has a common encryption software database, which is totally different in concept from the present invention.

Regarding Section 19:

Figure 3 of Schier illustrates a selected portion of one embodiment of encryption table 28 which is shown in Figure 2 of Schier. Encryption selection table 28 comprises a key column 34, a first algorithm column 36, a second algorithm column 38 and a third algorithm column 40. In operation, a particular device as device 14 would have the capability of performing a number of distinct encryption processes. For example, device 14 may be able to perform five different encryption techniques. An encryption key in key column 34 is then used to access a particular row which specifies a particular encryption technique in each of columns 36, 38 and 40. A message to be sent by device 14 or received by device 14 can then be encrypted or decrypted using the technique specified in the row in the order specified in the row. For example, if encryption key 51 is specified, the device 14 would first apply encryption algorithm 4, then encryption algorithm 3, then encryption algorithm 1. Conversely, if a message was received by device 14 and the key value 51 was to be used, the device 14 would first decrypt using algorithm 1 then decrypt using algorithm 3 followed by decryption using algorithm 4. In this manner, a number of relatively simple encryption steps can be sequentially applied to a message to greatly enhance the security of the message. A person attempting to intercept and wrongfully decrypt the message would have to discern not only the various kinds encryption used, but also the order in which the technique were used.

Problems exist in the method of Schier in that if encryption key 51 is specified, the device 14 would first apply encryption algorithm 4, then encryption algorithm 3, then encryption algorithm 1. Conversely, if a message was received by device 14 and the key value 51 was to be used, the device 14 would first decrypt using algorithm 1 then decrypt using algorithm 3 followed by decryption using algorithm 4.

The encryption algorithm in device 14 and the decryption algorithm in device 14 of Schier are not divided. This shows that the symmetric property of cryptocommunication is accepted unconditionally, which is much different from the present invention.

Existence of those who can return only a plaintext even if code data is receivable, and those who can return only the data which carried out weak encryption even if the data which gave the powerful code is receivable, is disregarded in the method of Schier.

Further, note that a legal issue may exist in the method of Schier which requires common encryption software, which may be a problem for users in some countries.

Still further, a correspondence table in accordance with the present invention provides a decryption portion in the form where it becomes independent. The method of Schier does not teach or suggest such a decryption portion.

Regarding Section 20:

The presently claimed invention in which the individual has an extended address book and in which the item of a name, the address, encryption software, an enciphering key, decryption software, and a decryption key exists as an item in the extended address book is not taught or suggested in the method of Vidrascu.

Regarding Section 21:

The presently claimed invention in which the individual has an extended address book and in which the item of a name, the address, encryption software, an enciphering key, decryption software, and a decryption key exists as an item in the extended address book is not taught or suggested in the combined method of Vidrascu, Leppek, Collins and Schier.

Regarding Section 23:

Leppek does not explain how object 160 in Figure 2 is generated from encr.key. In more detail, The way the structure of supervisory encryption manager is indefinite and generates object 160 from a key (encr.key) is not described at all in Leppek. One of ordinary skill in the art cannot determine what encr.key is, since it is not explained in Leppek.

The following questions exist from Leppek, whereby Leppek does not provide any suggestion of an answer.

1) When a new participant participates in this cryptocommunication network, can supervisory encryption manager be responded?

2) Supposing it can respond, what kind of train 160 will be generated to the participant who added newly?

3) How does a new participant obtain the encryption software registered into encryption operation data base?

4) How does a new participant obtain the encryption software registered into decryption operation data base?

In Table 100 of Leppek, separation of encryption software and an enciphering key is not made. Therefore, assuming that this database has to store the enciphering key, the

number of the encryption software which must be registered into a database increases to a tremendous amount, making it unfeasible.

In contrast, the extended address book according to the present invention solves such problems that exist in Leppek.

Regarding Section 26:

In column 6, lines 21-27 of Vidrascu, when IP data transmission transporting a TCP or UDP protocol is received (normally plane) on the interface 30 (See Figure 1 of Vidrascu), and if the keys related to the IP addresses of the sender and of the receiver are found, a part of the user data of this transmission is enciphered with a DES algorithm by using a key related to the IP address of the sender. The transmission is next sent to the interface 31.

In Vidrascu, the meaning of an IP address provides a problem all in itself. "user21@domain2" and "user22@domain2" belong to the same mail server with a same IP address, and also from "user11@domain1" to "user21@domain2". The same encryption is done in the communication from "user11@domain1" to "user21@domain2" and the communication from "user12@domain1" to "user22@domain2".

There are many people using the same provider's mail server, and the users using the same IP address increase in number inevitably over time. Therefore, with the same method and the same enciphering key, a lot of data will be enciphered and will be transmitted, whereby that date will be decoded at the other end.

The response between IP addresses means the response between mail servers. Now, it will be only a manager of a mail server that encryption software can be changed. There are typically many people using the same provider's mail server. The group of the people using two mail servers of them will use the same encryption software. Now, each user of an e-mail cannot change encryption software freely. It must be able to change quickly.

In order for the user of an E-mail to choose the encryption software which suited itself and to use freely, not according to the response of an IP address and an IP address but according to the response between mail addresses, encryption software, an enciphering key, decryption software, and a decryption key must be able to be set up freely.

If this is not made, cryptocommunication with those who live in the foreign countries where legal limits differ may cause legal problems for users. For realizing people of various countries registered into their own address book, and smooth cryptocommunication, the user

of an e-mail has to be able to set up finely freely in his own address book, which becomes a problem.

The present invention overcomes these problems of Vidrascu, by utilizing the item of a name, the address, encryption software, an enciphering key, decryption software, and a decryption key in an extended address book.

Leppek describes a virtual encryption scheme that involves the generation of a sequence of the access code, with immediately successive ones of the access code of the sequence being different from one another. Leppek does not rectify the problems of Vidrascu as identified above.

In Collins, the Internet e-mail gateway 240 converts the SMS message 100 to an Internet e-mail message having the format 150. To accomplish this, the Internet e-mail gateway 240 determines an Internet e-mail address for the cellular telephone 210 and for the Internet station 280. Regarding the Internet e-mail address for the cellular telephone 210, the Internet e-mail gateway 240 adds the domain name for the Internet e-mail gateway 240 to the SMS address for the cellular telephone located in the sender SMS address field 110 of the SMS message. To determine the Internet e-mail address for the Internet Station 280, the Internet e-mail gateway 240 uses a messaging service lookup table having a first column with a list of SMS addresses, where each SMS address corresponds to an Internet e-mail address in a second column of the lookup table. The Internet e-mail gateway 240 locates the SMS address of the Internet station 280 in the first column of the lookup table. The Internet e-mail address for the Internet station 280 is retrieved from the second column of the lookup table at a location corresponding to the Internet station SMS address of the first column.

In Collins, the SMS address, conversion of Internet e-mail address, and changing portable mail into an Internet mail are described. The mechanism in which the portable mail accepted only in the narrow range circulates in the whole world through the Internet by this is solved. In this regard, Collins does not rectify the problems of Vidrascu as identified above.

In Keats, it describes that each network element has its own SID (maintained for example in a memory element under control of the SID manager) and also maintains a database, table or other suitable structure in another memory element, such as a cache, which maps TIDs to IP address for IP connections from the particular network element to another network element in the network, as described in detail below. In this regard, Keats does not rectify the problems of Vidrascu as identified above.

Accordingly, the presently pending claims are patentable over the combined teachings of the cited art of record.

Regarding Section 28:

By the method of Leppek, the database for encryption exists, the operation for the encryption used out of it is selected, and in order to determine the sequence which applies it, 160 is generated and used. By this method, all the people that participate in a cryptocommunication network have to have a common code database.

Leppek begs the questions of how a common database is distributed to a new participant, and who does the distribution? For some countries, export and import of codes have a strong limit, the person who received the code database becomes an offender only by it, or the person of the way who sent becomes an offender.

If it is the database which collected only extremely weak codes, it may be able to distribute all over the world, but now, it does not become useful.

The retrieving table for pulling out the code operation used from a database itself contains the still bigger problem. Since the portion of the enciphering key to be used does not exist, it is considered to have registered into the retrieving table what had encryption software and an enciphering key.

The length of a safe key becomes still longer. If the length of a key becomes about 4000 bits, a table will overflow from a typical hard disk.

Thus, it is not useful to use a code database common provided to the whole, as taught by Leppek.

The present invention does not have these problems associated with Leppek.

Conclusion:

Since all of the issues raised in the Office Action have been addressed in this Amendment and Reply, Applicant believes that the present application is now in condition for allowance, and an early indication of allowance is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check or credit card payment form being in the wrong amount, unsigned, post-dated,

otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date October 13, 2006

By Phillip J. Articola

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (202) 672-5485
Facsimile: (202) 672-5399

William T. Ellis
Registration No. 26,874

Phillip J. Articola
Registration No. 38,819